

Ser. No. 09/998,082

Page 5 of 9

REMARKS

Claims 1 through 15 are pending. Claim 1 stands rejected under 35 U.S.C. 101 as lacking utility. Claims 1-5 and 8-15 stand rejected under 35 U.S.C. 102(e) as anticipated by each of Philips and Tagawa. Claims 6 and 7 are indicated to be allowable if rewritten in independent form including all of the limitations of the base and intervening claims.

35 U.S.C. 101 rejection of claim 1

Claim 1 has been amended to recite

"A processor-implemented method
identifying content to be downloaded by inputting the content to a
processing device;
partitioning the content using a program executed by the processing
device."

Thus, Claim 1, as amended, defines structural and functional interrelationships between data structures and a processing device. Withdrawal of the 35 U.S.C. 101 rejection is respectfully requested.

35 USC 102 (e) rejection of claims 1-5 and 8-15 in view of Phillips and Tagawa

As shown below, Philips and Tagawa neither teach nor suggest downloading an illicit content material by partitioning the content material into section *each having a duration less than a threshold duration value assigned by a screening algorithm*, as recited in independent claims 1, 14 and 15.

PHILIPS

The Examiner states that Philips discloses "[P]artitioning the content into at least two section wherein each ... has a duration ... less than a threshold duration value assigned by the screening algorithm (see., abstract, pages 1-8)." (See Office Action, page 3, section 8) The Examiner is incorrect, with all due respect.

Philips discloses downloading of a legitimate content material which is encrypted by using a unique identification code of a given device. The material is then decrypted "using a decryption key that is based on the identification code." (See Philips, Abstract) The material to be downloaded, a track, "is intended to refer to any pre-recorded fixed

BEST AVAILABLE COPY

Ser. No. 09/998,082

Page 6 of 9

segment of audio or video content.” (See Philips, page 2, paragraph 0025) Clearly, no partitioning of the pre-recorded fixed segment is taught by the above-referred passages of Philips’s disclosure. In contrast, claim 1 of the invention recites partitioning the content into sections.

On page 4, paragraph 0048, Philips discloses that “the playing by media player 102 will essentially involve reading such digital data and performing any necessary processing, such as decompression (in certain cases), error detection/correction, and/or implementing any security features.” Nothing here teaches what “any security features” may include. More importantly, the text on page 4 is absolutely silent about partitioning a track into sections each having a duration less than a duration value assigned by an algorithm, as recited in claim 1 of the invention.

Skipping pages 5-7 that do not provide a teaching regarding security measures, Applicants direct the Examiner’s attention to page 8 of Philips disclosing the operation of Philip’s device. In particular, paragraph 0090 discloses that a track to be downloaded is encrypted so that it only can be decrypted “using the unique decryption key corresponding to the specific system 100.” The downloaded track can be then decrypted by using symmetric or asymmetric encryption. Again, no teaching is provided as to partitioning an illicit content into sections each having a duration less than a reference value assigned by an algorithm. In contrast, claim 1 of the invention recites partitioning of content material into sections so that each section lasts less than a threshold duration value assigned by a securing algorithm.

Accordingly, Philips does not have all of the elements recited in claim 1, which is, thus, patentable over Philips.

Claims 2-5 and 8-13 depend from claim 1 and, thus, are patentable, too.

Claims 14 and 15, as mentioned above, each recite the subject matter discussed above in reference to claim 1 and, thus, are patentable over Philips.

TAGAWA et al.

Tagawa discloses a recording method for reproducing legitimate digital data that may carry watermarks and for protecting the data’s copyrights. (See Tagawa, page 1, paragraph 0011, page 8, paragraph 0121) Initially, the digital data is downloaded in a data recording apparatus, such as a PC, and stored in its hard disc. (See Tagawa, page 4,

BEST AVAILABLE COPY

Ser. No. 09/998,082

Page 7 of 9

paragraph 0069; page 5, paragraph 0080) The stored data is further decrypted by using the data provider's decryption key.

The decrypted data is re-encrypted by obtaining an inherent information of a secondary recording medium 114, including a combination of a DVD-Ram disc and a small-scale memory, which is coupled to a recording unit 115, such as a DVD-Audio player of the data recording apparatus. Re-encryption includes creating and recording a unique encryption key based on the inherent information associated with secondary recording medium 114. If the inherent information is not obtainable, the decrypted data cannot be re-encrypted and, therefore, cannot be recorded on secondary recording medium 114. "As a result, if a user with a malicious intent makes a copy of the content of the DVD-RAM disc on another recording medium by using a tool for a bit copy and tries to play back the copied data on other recording media, the copied data cannot be normally decrypted since the information corresponding to the decryption key of the other recording medium is different from that of the DVD-RAM disc." (See Tagawa, page 6, paragraph 0092)

The unique encryption key further includes an inherent information embedded in recording unit 115 used during the original recording. As a result, secondary recording medium 114 can be played only by originally used recording unit 115. (See Tagawa, page 6, paragraph 0093) Note that the above-discussed principle of operation is applicable to all of the Tagawa's embodiments disclosed on pages 1-16.

Thus, Tagawa does not teach a security mechanism requiring partitioning content material into sections each of which lasts for a period of time shorter than a reference time period assigned to a security algorithm, as recited in claim 1 of the invention. To circumvent the security mechanism of Tagawa and download a data, one needs to obtain an inherent information of originally used DVD-Rams and DVD players. Accordingly, Claim 1 is patentable over Tagawa since the cited prior art reference does not have all of the elements recited in claim 1.

Claims 2-5 and 8-13 depend from claim 1 and benefit from its patentability. Independent claims 14 and 15 each recite a structure operative to identify content and partition the content into sections each of which lasts less than a predetermined period of time assigned by a screening algorithm. As has been discussed above, Tagawa neither

BEST AVAILABLE COPY

Ser. No. 09/998,082

Page 8 of 9

teaches nor suggests such a structure. Accordingly, claims 14 and 15 are patentable over Tagawa.

In summary, Philips and Tagawa, individually, do not have all the elements as recited in the claims of the invention, and, therefore, do not anticipate the claims. Reconsideration and withdrawal of the 35 U.S.C. 102(e) rejection of claims 1-5 and 8-15 are in order.

Conclusion

Based on all of the above, it is respectfully submitted that the present application is now in proper condition for allowance. Prompt and favorable action to this effect, and early passing of this application to issue, are respectfully solicited.


Note that no new issue has been introduced into amended claims, and, therefore, no search is needed.

Claims 6 and 7 indicated to be allowable remain dependent from claim 1.

Should the Examiner have any comments, questions, suggestions or objections, the Examiner is respectfully requested to telephone the undersigned in order to facilitate reaching a resolution of any outstanding issues.

Additional fees required for two extra independent may be charged to our Patent and Trademark Office Deposit Account No. 14-1270.

Respectfully submitted,

By 
Yuri Kateshov, Reg. No. 34,466
914-723-6802

BEST AVAILABLE COPY